acunetix

Developer Report

Acunetix Security Audit

26 August 2021

Generated by Acunetix

Scan of thachban.vaccom.vn

Scan details

Scan information	
Start time	25/08/2021, 06:33:40
Start url	https://thachban.vaccom.vn
Host	thachban.vaccom.vn
Scan time	4 minutes, 13 seconds
Profile	Full Scan
Server information	nginx/1.21.1
Responsive	True
Server OS	Unknown

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	4
High	0
Medium	1
Low	1
Informational	2

Alerts summary

TLS 1.0 enabled

Classification	
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 3.1 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-16

Affected items	Variation
Web Server	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693

Affected items	Variation
Web Server	1

Content Security Policy (CSP) not implemented

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

TLS 1.1 enabled

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

Alerts details

TLS 1.0 enabled

Severity	**Medium**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The web server supports encryption through TLS 1.0. TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Recommendation

It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

References

Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)
PCI 3.1 and TLS 1.2 (Cloudflare Support) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

Affected items

Web Server
Details
The SSL server (port: 443) encrypts traffic using TLSv1.0.
Request headers

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Reported by module	/Scripts/PerServer/Clickjacking_X_Frame_Options.script

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)
Clickjacking (https://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)
Defending with Content Security Policy frame-ancestors directive (https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)
Frame Buster Buster (https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server
Details
Request headers

```
GET / HTTP/1.1
Cookie:
Token=eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0aHV5Y3QiLCJpYXQiOjE2Mjk4NzU4NTcsImV4cCI6MTYyOTkxMTg1N30.KiNru9R_KTK9hiErvQkS6z6hRWh-6VT9qBtNd5OZir-magGhLihwHxpdLEb99AZydlucWvU_twoPbCi2cyd-Dg
Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0aHV5Y3QiLCJpYXQiOjE2Mjk4NzU4NTcsImV4cCI6MTYyOTkxMTg1N30.KiNru9R_KTK9hiErvQkS6z6hRWh-6VT9qBtNd5OZir-magGhLihwHxpdLEb99AZydlucWvU_twoPbCi2cyd-Dg
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: thachban.vaccom.vn
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Content Security Policy (CSP) not implemented

Severity	**Informational**
Reported by module	/httpdata/CSP_not_implemented.js

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details
Request headers

```
GET / HTTP/1.1
Referer: https://thachban.vaccom.vn/
Cookie:
Token=eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0aHV5Y3QiLCJpYXQiOjE2Mjk4NzU4NTcsImV4cCI6MTYyOTkxMTg1N30.KiNru9R_KTK9hiErvQkS6z6hRWh-6VT9qBtNd5OZir-magGhLihwHxpdLEb99AZydlucWvU_twoPbCi2cyd-Dg
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0aHV5Y3QiLCJpYXQiOjE2Mjk4NzU4NTcsImV4cCI6MTYyOTkxMTg1N30.KiNru9R_KTK9hiErvQkS6z6hRWh-6VT9qBtNd5OZir-magGhLihwHxpdLEb99AZydlucWvU_twoPbCi2cyd-Dg
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: thachban.vaccom.vn
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

TLS 1.1 enabled

Severity	**Informational**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The web server supports encryption through TLS 1.1. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended (although at the time or writing not required) to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Recommendation

It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.

References

Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)
PCI 3.1 and TLS 1.2 (Cloudflare Support) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

Affected items

Web Server
Details
The SSL server (port: 443) encrypts traffic using TLSv1.1.
Request headers

Scanned items (coverage report)

https://thachban.vaccom.vn/
https://thachban.vaccom.vn/images/
https://thachban.vaccom.vn/js/
https://thachban.vaccom.vn/vac/
https://thachban.vaccom.vn/vac/css/
https://thachban.vaccom.vn/vac/css/app.096d37c1.css
https://thachban.vaccom.vn/vac/css/chunk-1aa81273.fea47a87.css
https://thachban.vaccom.vn/vac/css/chunk-28062148.f4f2c1ce.css
https://thachban.vaccom.vn/vac/css/chunk-2ddb732e.802e53b9.css
https://thachban.vaccom.vn/vac/css/chunk-336d637e.4fd899df.css
https://thachban.vaccom.vn/vac/css/chunk-403eea34.843844df.css
https://thachban.vaccom.vn/vac/css/chunk-46e90e46.3cadf264.css
https://thachban.vaccom.vn/vac/css/chunk-4e1f0266.9b8f39b5.css
https://thachban.vaccom.vn/vac/css/chunk-5a7ebdf0.8bfbe84b.css
https://thachban.vaccom.vn/vac/css/chunk-5eb439b2.689bcdfe.css
https://thachban.vaccom.vn/vac/css/chunk-61da2064.ace1abdd.css
https://thachban.vaccom.vn/vac/css/chunk-719b6c4f.18ee62d6.css
https://thachban.vaccom.vn/vac/css/chunk-72504ee2.160aed52.css
https://thachban.vaccom.vn/vac/css/chunk-7283eb0c.ce726831.css
https://thachban.vaccom.vn/vac/css/chunk-7f705276.8db3930b.css
https://thachban.vaccom.vn/vac/css/chunk-c1676726.c23c9764.css
https://thachban.vaccom.vn/vac/css/chunk-c8ee7aa4.b05239b4.css
https://thachban.vaccom.vn/vac/css/chunk-e2fa2df0.d66cd414.css
https://thachban.vaccom.vn/vac/css/chunk-f4ee3704.df5c9211.css
https://thachban.vaccom.vn/vac/css/chunk-vendors.a3629002.css
https://thachban.vaccom.vn/vac/images/
https://thachban.vaccom.vn/vac/js/
https://thachban.vaccom.vn/vac/js/app.9cdb62f2.js
https://thachban.vaccom.vn/vac/js/chunk-1aa81273.20d17914.js
https://thachban.vaccom.vn/vac/js/chunk-28062148.9f75418a.js
https://thachban.vaccom.vn/vac/js/chunk-2d0d32d2.efd0394d.js
https://thachban.vaccom.vn/vac/js/chunk-2d221fbb.891406fe.js
https://thachban.vaccom.vn/vac/js/chunk-2ddb732e.20242e65.js
https://thachban.vaccom.vn/vac/js/chunk-336d637e.a2e30e57.js
https://thachban.vaccom.vn/vac/js/chunk-34136339.943d6183.js
https://thachban.vaccom.vn/vac/js/chunk-403eea34.5539a3fa.js
https://thachban.vaccom.vn/vac/js/chunk-46e90e46.14d87869.js
https://thachban.vaccom.vn/vac/js/chunk-4e1f0266.062bd5ec.js
https://thachban.vaccom.vn/vac/js/chunk-5a7ebdf0.f93b63b9.js
https://thachban.vaccom.vn/vac/js/chunk-5eb439b2.a28f6e37.js
https://thachban.vaccom.vn/vac/js/chunk-61da2064.7cf3c77d.js
https://thachban.vaccom.vn/vac/js/chunk-719b6c4f.9304cbc4.js
https://thachban.vaccom.vn/vac/js/chunk-72504ee2.5e537fd1.js
https://thachban.vaccom.vn/vac/js/chunk-7283eb0c.36cceb34.js
https://thachban.vaccom.vn/vac/js/chunk-7f705276.4913c1b3.js
https://thachban.vaccom.vn/vac/js/chunk-c1676726.694b0d1c.js
https://thachban.vaccom.vn/vac/js/chunk-c8ee7aa4.b8085e8c.js
https://thachban.vaccom.vn/vac/js/chunk-e2fa2df0.ed9f2208.js
https://thachban.vaccom.vn/vac/js/chunk-f4ee3704.38d2366b.js
https://thachban.vaccom.vn/vac/js/chunk-vendors.05233130.js